CLAIMS

WHAT IS CLAIMED:

1. A computer system, comprising:

a peripheral device;

a processing unit adapted to execute a driver for interfacing with the peripheral device in a standard mode of operation and an authentication agent in a privileged mode of operation, wherein the authentication agent includes program instructions adapted to authenticate the driver.

2. The system of claim 1, wherein the authentication agent includes program instructions adapted to signal a security violation in response to a driver authentication failure.

3. The system of claim 1, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the driver, decrypt a digest associated with the driver, and compare the hash to the digest to authenticate the driver.

4. The system of claim 3, wherein the authentication agent includes program instructions adapted to decrypt the digest associated with the driver using a public key.

5. The system of claim 1, wherein the processing unit includes a timer adapted to generate an interrupt signal for invoking the authentication agent after a predetermined interval.

6. The system of claim 1, wherein the driver includes program instructions adapted to periodically invoke the authentication agent.

7. The system of claim 1, wherein the privileged mode of operation comprises a system management mode of operation.

8. The system of claim 1, wherein the driver includes program instructions adapted to issue a signal to the processing unit to initiate a change from the standard mode of operation to the privileged mode of operation.

9. The system of claim 8, wherein the signal comprises a system management interrupt.

10. The system of claim 1, further comprising a system basic input output system (BIOS) memory adapted to store the authentication agent.

11. The system of claim 10, wherein the processing unit is adapted to load the authentication agent from the system BIOS into a protected memory location during initialization of the computer system.

12. The system of claim 11, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver using a public key, and compare the hash to the digest to authenticate the modem driver, and the system further comprises a system basic input output system (BIOS) memory adapted to store the public key.

13. The system of claim 1, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver using a public key, and compare the hash to the digest to authenticate the modem driver, and the peripheral device includes a memory device adapted to store the public key.

14. The system of claim 2, wherein the authentication agent includes program instructions adapted to prohibit further operation of the driver in response to identifying the security violation.

15. The system of claim 1, wherein the authentication agent includes program instructions adapted to prohibit further operation of the processing unit in response to identifying the security violation.

16. A communications system, comprising:

a physical layer hardware unit adapted to communicate data over a communications channel in accordance with assigned transmission parameters, the physical layer hardware unit being adapted to receive an incoming signal over the communications channel and sample the incoming signal to generate a digital received signal; and

a processing unit adapted to execute a modem driver in a standard mode of operation and an authentication agent in a privileged mode of operation, wherein the standard mode driver includes program instructions adapted to extract control codes from the digital received signal and configure the physical layer

hardware assigned transmission parameters based on the control codes, and the authentication agent includes program instructions adapted to authenticate the modem driver

17. The system of claim 16, wherein the authentication agent includes program instructions adapted to signal a security violation in response to a modem driver authentication failure.

18. The system of claim 16, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver, and compare the hash to the digest to authenticate the modem driver.

19. The system of claim 18, wherein the authentication agent includes program instructions adapted to decrypt the digest associated with the modem driver using a public key.

20. The system of claim 16, wherein the processing unit includes a timer adapted to generate an interrupt signal for invoking the authentication agent after a predetermined interval.

21. The system of claim 16, wherein the modem driver includes program instructions adapted to periodically invoke the authentication agent.

22. The system of claim 16, wherein the transmission assignments include at least one of a power level assignment, a frequency assignment, and a time slot assignment.

23. The system of claim 16, wherein the privileged mode of operation comprises a system management mode of operation.

24. The system of claim 16, wherein the modem driver includes program instructions adapted to issue a signal to the processing unit to initiate a change from the standard mode of operation to the privileged mode of operation.

25. The system of claim 24, wherein the signal comprises a system management interrupt.

26. The system of claim 16, wherein the processing unit comprises a computer.

27. The system of claim 26, wherein the computer includes:

a processor complex adapted to execute the program instructions in the modem driver and the authentication agent;

a bus coupled to the processor complex; and

an expansion card coupled to the bus, the expansion card including the physical layer hardware.

28. The system of claim 26, wherein the computer includes a system basic input output system (BIOS) memory adapted to store the authentication agent.

29. The system of claim 28, wherein the computer is adapted to load the privileged mode driver from the system BIOS into a protected memory location during initialization of the computer.

30. The system of claim 26, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver using a public key, and compare the hash to the digest to authenticate the modem driver, and the computer further comprises a system basic input output system (BIOS) memory adapted to store the public key.

31. The system of claim 27, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver using a public key, and compare the hash to the digest to authenticate the modem driver, and the expansion card includes a memory device adapted to store the public key.

32. The system of claim 17, wherein the authentication agent includes program instructions adapted to prohibit further operation of the modem driver in response to identifying the security violation.

33. The system of claim 16, wherein the authentication agent includes program instructions adapted to prohibit further operation of the processing unit in response to identifying the security violation.

34. A method for identifying security violations in a computer system, comprising:

executing a driver in a standard processing mode of a processing unit;

transitioning the processing unit into a privileged processing mode; and

authenticating the driver in the privileged processing mode.

35. The method of claim 34, further comprising signaling a security violation in response to a driver authentication failure.

36. The method of claim 34, wherein authenticating the driver includes:

generating a hash of at least a portion of the driver;

decrypting a digest associated with the driver; and

comparing the hash to the digest to authenticate the driver.

37. The method of claim 36, wherein decrypting the digest comprises decrypting the digest using a public key.

38. The method of claim 34, further comprising generating an interrupt signal for authenticating the driver in the privileged processing mode after a predetermined interval.

39. The method of claim 35, further comprising prohibiting further operation of the driver in response to identifying the security violation.

40. The method of claim 35, further comprising prohibiting further operation of the processing unit in response to identifying the security violation.

41. A system for identifying security violations, comprising:

means for executing a driver in a standard processing mode of a processing unit;

means for transitioning the processing unit into a privileged processing mode; and

means for authenticating the driver in the privileged processing mode.